telephones, and ledgers containing code numbers, customers and stash locations, all of which facilitate drug distribution;

h. when drug traffickers amass significant proceeds from the sale of drugs, they attempt to legitimize these profits through money laundering activities. To accomplish these goals, drug traffickers utilize, among other mechanisms, domestic and international banks and their attendant accounts, casinos, real estate, shell corporations and business fronts, and otherwise legitimate businesses, which generate large quantities of currency. Traffickers often commingle narcotics proceeds with money generated by legitimate businesses;

i. narcotics traffickers at times become fearful that their extravagant spending habits will bring them under scrutiny by the Internal Revenue Service or other federal, state, or local agencies. In order to legitimize their spending, these traffickers file tax returns reporting income commensurate with the amount of money they have spent during the year which they feel can be traced and documented by the government. The source of their income reported on these returns is usually falsely stated, misleading or generic in terms. Retained copies of these returns are commonly kept by the traffickers in their residences, businesses, on their computers, and in other secure locations;

j. traffickers commonly maintain books or papers which reflect names, addresses and/or telephone numbers of their associates in the trafficking organization;

k. traffickers keep photographs of themselves, their associates, and their property in their cellular telephones and computers.

11. In my training and experience, I know it is common for persons involved in drug trafficking and suspicious financial activities to maintain records of their activities, such as ledgers, bank account records, contact information for co-conspirators, drug proceeds, books, records, receipts, notes, emails, ledgers, airline tickets, receipts relating to the purchase of financial instruments and or the transfer of funds, and other papers relating to the transportation, ordering, sale and distribution of controlled substances. Furthermore, in my training and experience, I have learned that it is common for persons involved in drug trafficking and money laundering to store these items in

their cellular telephones, computers, cameras, and electronic devices frequently used in furtherance of their drug trafficking and money laundering activities.

12. Based on my training and experience, the evidence recovered from the above-described search of DION's office and the evidence previously recovered from DION's truck at the time of his arrest (including a number of computer-generated documents and records), I believe that documents, records, videos, photographs, and other evidence of drug trafficking and money-laundering activities will be found on the Target Devices.

SEIZURE OF COMPUTER EQUIPMENT AND DATA

13. Based on my knowledge and training and the experience of other agents with whom I have spoken, I know that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer equipment, software, peripherals, and related documentation be seized and subsequently processed by a qualified computer specialist in a laboratory setting. This is true because of the following:

14. The volume of evidence. Computer storage devices (such as hard disks, flash drives, magnetic and optical disks) can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This sorting process can take weeks or

months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

15. Technical requirements. Analyzing computer systems for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, password-protected, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction (both from external sources and destructive code imbedded in the system as a "booby trap").

16. In light of the volume of data at issue and these technical requirements, it is generally necessary that data, hardware, software, and storage media, be seized and subsequently processed by a qualified computer specialist in a laboratory setting rather than in the location where it is seized. It is also generally necessary for agents to seize most or all of a computer system's input/output peripheral devices, software, and computer-related documentation, in order for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment.

17. Attachments B, C and D to the proposed warrant, which contain sections relating to the search and seizure of computer equipment and data, are appended to my

Affidavit and incorporated by reference.

CONCLUSION

18. Based on all of the foregoing, I believe that on and in the property described above as the Target Devices, more fully described in Attachment A, there is probable cause to believe that the items set forth in Attachment C will be found.

I declare that the foregoing is true and correct to the best of my knowledge and belief.

SA/FBI

Special Agent Stephen J. Kelleher
Federal Bureau of Investigation

Subscribed and sworn to before me this 30th day of October, 2013.

Marianne B. Bowler, USMJ

HONORABLE MARIANNE B. BOWLER
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF MASSACHUSETTS

ATTACHMENT A
ITEMS TO BE SEARCHED

Description	Referred to herein as
1. 22 floppy discs seized from Marshall Dion's office, located at 4 Longfellow Place, Suite 3802, Boston, Massachusetts on October 25, 2013	Target Storage Device
2. A red Nokia cellular telephone, bearing ESN 11416590728	Target Telephone; Photograph in Attachment A
3. A Centon 16GB USB flash drive seized from Marshall Dion's office, located at 4 Longfellow Place, Suite 3802, Boston, Massachusetts on October 25, 2013	Target Storage Device; Photograph in Attachment A
4. A Seagate Momentus 320GB hard drive, bearing serial no. 5VE43GWP	Target Storage Device; Photograph in Attachment A
5. A Seagate Momentus 160GB hard drive, bearing serial no. 5NK0ZXFS	Target Storage Device; Photograph in Attachment A
6. An Eagle 750GB external computer drive, bearing serial no. ABG10160170	Target Storage Device; Photograph in Attachment A
7. A Seagate hard drive, bearing serial no. JE105518	Target Storage Device; Photograph in Attachment A
8. A Maxtor 200GB hard drive, bearing serial no. B417C8TH	Target Storage Device; Photograph in Attachment A

ATTACHMENT B
DEFINITIONS

For the purpose of this Warrant:

1. "Computer hardware" means: electronic devices capable of data processing (such as laptop and desktop computers, personal digital assistants ("PDAs"), and wireless communication devices); peripheral input/output devices (such as keyboards, printers, scanners, monitors, and drives intended for removable storage media); related communications devices (such as wireless cards, modems, cables, and connections), and security devices, (such as electronic data security hardware and physical locks and keys).

2. "Computer software" means: programs, program codes, information and data stored in any form (such as operating systems, applications, utilities, communications and data security software; log, history and backup files; encryption codes; user names; and passwords), whether deliberately, inadvertently, or automatically stored.

3. "Computer-related documentation" means: any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

4. "Storage media" means: any media capable of collecting, storing, retrieving, or transmitting data (such as hard disks, floppy disks, CDs, DVDs, tapes, USB flash drives and memory cards).

5. "Data" means: all information stored on storage media of any form (such as documents, tables, metadata, audio and visual files, their drafts and their modifications, whether deliberately, inadvertently, or automatically stored).

6. "A Record" is: any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

ATTACHMENT C

ITEMS TO BE SEIZED

A. All records, in whatever form, and tangible objects that constitute evidence, fruits, and/or instrumentalities of drug distribution and money laundering, as set forth below:

1. Records of personal or business activities relating to the operation or ownership of any computer hardware, software, storage media, or data (such as user names, passwords, telephone records, notes, books, diaries, and reference materials).

2. Records pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media.

3. Records relating to ownership, occupancy, or use of the premises searched (such as utility bills, phone bills, rent payments, mortgage payments, photographs, insurance documentation, receipts and check registers).

4. Records relating to drugs, drug proceeds, drug distribution, drug importation, money laundering, money transfers, ledgers, contact lists, price sheets, and related documents.

5. Records and information identifying contact information for co-conspirators, communications made in furtherance of the conspiracy, and photographs and videos of co-conspirators.

B. All computer hardware; computer software; computer-related documentation; and storage media. Off-site searching of such hardware, software, documentation, and storage media, shall be limited to searching for the items described in paragraph A of this attachment and shall be done according to the procedures set out in Attachment D.

ATTACHMENT D

PROCEDURES FOR SEIZING COMPUTERS AND RELATED DEVICES

1. Seizing hardware and software

Agents are authorized to seize and remove from the premises the computer hardware, software, related documentation, and storage media, so that computer analysts can accurately retrieve the items authorized by this warrant in a laboratory or other controlled environment. The retrieval process does not need to be completed within 10 days after the date of the warrant or before the return of the written inventory required by Fed. R. Crim. P. 41(a).

2. Returning hardware and software

If, after inspecting a seized computer system, the agents and computer analysts determine that these items are no longer necessary to retrieve and preserve electronic evidence, the prosecutor determines that they need not be preserved as evidence, fruits or instrumentalities of a crime, and these items do not contain contraband, they should be returned within a reasonable time, upon written request.

If the computer system cannot be returned, agents should, upon written request, make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that are neither the fruits nor instrumentalities of crime nor contraband.

[redacted]

25/2
3 -
arch
rrant
4
gfell
w
ace,
uite
02,
ston
IA

Evid
ence
Inve
ntory
List
of
Mars
hall
Dion'
s
Offic
e

Item #	Location	Agent/Officer	Description
1	Room A	Kelleher	1 Fleet Bank checkbook; various manilla envelopes containing floppy dis
2	Room A	Bulman	Assort
3	Room A	Kelleher	

4	Room A	Bulman	Financial documents; magazine clippings; letters
5	Room A	McDermott	Car re
6	Room A	McDermott	1 red Nokia cellular telephone (ESN: 11416
7	Room A	McDermott	1 brown bag containing money bands, typed labels such as "ALMOST NEW
8	Room A	McDermott	1 grey plastic bag containing 5 blue b
9	Room A	Kelleher	1 contact list; documents from Sovereign Bank, Bank of America, AT8
10	Room A	Bulman	
11	Room A	Bulman	1 Scan Coin cash counter.
12	Room A	Tiberi	1 box with financial documents from Bank of America
13	Room A	Tiberi	1 red plastic box containing documents from Sovereign Bank, Bank of Ame
14	Room A	Tiberi	1 Fluke
15	Room A	Bulman	Printout of Currency and Foreign Transactions Reporting Act; misc. docu
16	Room A	Tiberi	Misc. documents, ha
17	Room A	Tiberi	1 red bag containing various keys; financial documents from Bank of Ar
18	Room A	Bulman	1 grey plastic box containg wide range of documents, notes, spreadshe
19	Room A	McDermott	9 UPS shipping boxes with hand-writte
20	Room A	Kelleher	Contact list; e-mails from Jeanette Leighton; Sovereign Bank deposi
21	Room A	McDermott	Hand-written and copies of ledgers in manilla envelopes; cont
22	Room A	Tiberi	Documents for $3,000 wire transfer to Jeanette Leighton; shipping label
23	Room A	Bulman	Documents and copies of checks of payment for storage unit in Plym
24	Room A	McDermott	
25	Room A	Bulman	
26	Room A	Bulman	
27	Room A	Kelleher	1 Seagate internal computer drive, S/N: 5VE43GWP; 1 Seagate internal co
28	Room A	McDermott	6 Sovereign Bank checkbooks; 5 Bank of America checkbooks; 22 check r
29	Room A	McDermott	1 Eagle 750 GB externa
30	Room A	McDermott	1 Seagate internal computer drive, S/N: JE105518, 1 Maxtor internal com
31	Room A	McDermott	